GENERAL FINITE-FIELD MULTIPLIER AND METHOD OF THE SAME

BACKGROUND OF THE INVENTION

1. Field of the Invention

5   The present invention relates to the field of finite-field multipliers, and more particularly, to a general finite-field multiplier and the method of the same.

2. Description of Related Art

        A finite-field element is a value with a fixed bit number, for
10   example, an element has four bits, and thus 16 values are possibly formed. Since in the encryption or error correction (such as Reed-Solomon code, abbreviated as RS code), signals are necessary to be coded so that the coded value can be represented by a mathematical polynomial p(x) and then a decoded operation can be used. Therefore, each fixed bit value
15   must be given a representation symbol. Furthermore, the AND and XOR operations can be performed between these symbols for generating another symbols. For example, four bits are used as a symbol of an element. When AND or XOR operations are performed between different elements, at most only 16 results may be generated. Therefore,
20   the set of these symbols having four bits can be used as a finite field. Through the operations of these elements in the finite field, the data can be encrypted or decrypted, and coded or decoded.

        For the addition of two elements, it can be implemented by an XOR gate. However, to design the circuit for the multiplying operation of
25   two elements is more complex. Conventionally, the multiplying

1

operation is performed by a finite-field multiplier formed by, for example, a Berlekamp multiplier and two basis converters. This finite-field multiplier is known as a bit-serial multiplier. Therefore, the circuit structure is very simple. However, an obvious disadvantage is that the

5 speed of multiplying is very slow. Moreover, the specification of p(x) is formed by a constant form, and thus, it can not be adjusted according to the practical requirement.

In order to avoid the problem in that the speed of the multiplier is too slow, a parallel construction may be used. This parallel multiplier

10 primarily utilizes a Mastrovito finite-field multiplying operation, wherein one of two elements to be multiplied is at first converted to a matrix, and then vector-multiplied with the second element for generating a desired value. Therefore, the parallel multiplier is primarily formed by AND gates and XOR gates, and the components thereof are

15 increased with the highest order of m. Therefore, the complexity of the hardware is $O(m^2)$.

As such, the finite-field multiplier is improved from the conventional bit-serial multiplier into a parallel multiplier. Most of the design specification of the multiplier is constant. When the specification

20 of the p(x) is changed, the conventional constant-type p(x) can not be used. Therefore, Hasan disclosed an adjustable bit-serial systolic finite-field multiplier, wherein the p(x) is changeable. Fig. 6 shows a bit-serial systolic matrix generator of a finite-field element multiplier disclosed by Hasan, which is provided primarily for receiving an element

2

$A = (a_0, a_1, \cdots, a_{m-1})$ to generate a column vector for matrix operation, wherein columns 1 ~ m-1 will generate the column vector of the matrix, while the p(x) is changeable and can control the bit number of an element. The circuit structure of a combination component Q in this multiplier is illustrated in Fig. 7. There are three input values, wherein p_{in} is a series of coefficients input to the p(x). As the first bit value of the symbol is received, q_{in} will input an 1, otherwise a 0 , while a_{in} will generate the operation value in the matrix. The operation of the circuit is listed in the following:

if $q_{in} = 1$

then

$a_{out} = r$; $r = a_{in}$;

else

$g_{out} = g_{temp}$; $g_{temp} = g_{in}$;

$q_{out} = q_{temp}$; $q_{temp} = q_{in}$;

Fig. 8 shows a complete functional module of this multi-functional bit-serial multiplier. The circuit of the internal element W thereof is illustrated in Fig. 9. Therefore, in this multiplier, element Q is used as a synthetic circuit for embodying required values in the matrix operation, and then, together with the element W and several dozens of

3

flip-flops, the circuit of the multiplier can be accomplished. However, this circuit is only suitable for a finite-field multiplier with a constant length. In comparing with the aforesaid conventional multiplier with a constant $p(x)$, there are too many logic gates used. Therefore, the

5   disadvantage is that a large latency is employed in the data output of the circuit.

In the aforementioned conventional bit-serial multiplier, as a bit value is received, the shifting and multiplying operations must be performed for generating a desired value. The time of shifting for a

10   multiplying operation of two elements in the multiplier is related to the highest order of the $p(x)$ or is related to the number of bits interpreting a symbol. When the highest order of $p(X)$ becomes larger, although the conventional bit-serial multiplier has less logic gate delays, the output thereof is in a bit serial manner, which may cause a serious problem in the

15   computation of a Reed-Solomon code algorithm. Therefore, it is desirable to provide an improved general finite-field multiplier device and the method of the same to mitigate and/or obviate the aforementioned problems.

SUMMARY OF THE INVENTION

20   The object of the present invention is to provide a general finite-field multiplier and the method of the same, wherein a programmable multi-bit input and a programmable multi-bit multiplying operation are used, so that it can be integrated with a conventional system to provide a high convenience and it can be used in the RS chip for different

25   specifications.

In accordance with a first aspect of the present invention, there is provided a general finite-field multiplication method for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C. The method comprises: a step of generating a parallel column-based matrix vector for expanding A into a matrix form and sequentially generating each element in each column of said A matrix, wherein the elements have values of $A, A\alpha, A\alpha^2 \cdots A\alpha^{m-1}$, respectively; and a step of a parallel column-based vector multiplication operation for directly multiplying each element of each column of the matrix A, that is generated sequentially, with the vector B, and all the multiplication results are accumulated so as to acquire the vector C.

In accordance with a second aspect of the present invention, there is provided a general finite-field multiplication method for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C. The method comprises: a step of generating a parallel matrix vector for generating the values of the elements in all columns of said matrix A is at a time, wherein the values are $A, A\alpha, A\alpha^2 \cdots A\alpha^{m-1}$, respectively; and a step of parallel column-based vector multiplication operation for multiplying matrix A with said vector B when the matrix A is generated, so as to acquire the vector C.

In accordance with a third aspect of the present invention, there is provided a general finite-field multiplier for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C. The multiplier comprises: a parallel column-based

5

matrix vector generator for expanding A into a matrix form and sequentially generating each element in each column of said A matrix, wherein the elements have values of $A, A\alpha, A\alpha^2 \cdots A\alpha^{m-1}$, respectively; and a parallel column-based vector multiplication operator for directly multiplying each element of each column of the matrix A, that is generated sequentially, with the vector B, and all the multiplication results are accumulated so as to acquire the vector C.

In accordance with a fourth aspect of the present invention, there is provided a general finite-field multiplier for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C. The multiplier comprises: a parallel matrix vector generator for generating the values of the elements in all columns of said matrix A is at a time, wherein the values are $A, A\alpha, A\alpha^2 \cdots A\alpha^{m-1}$, respectively; and a parallel vector multiplication operator for multiplying matrix A with said vector B when the matrix A is generated, so as to acquire the vector C.

Other objects, advantages, and novel features of the invention will become more apparent from the following detailed description when taken in conjunction with the accompanying drawings.

20 BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a structure of a preferred embodiment of the finite-field multiplier according to the present invention.

FIG. 2 shows a circuit of the finite-field multiplier illustrated in Fig. 1.

25 Fig. 3 shows a structure of another preferred embodiment of the

6

finite-field multiplier according to the present invention.

Fig. 4 is a circuit diagram of a parallel matrix vector generator illustrated in Fig. 3.

Fig. 5 is a circuit diagram of the parallel vector multiplication operator of the present invention.

Fig. 6 is a matrix generator of a conventional Hasan finite-field multiplier.

Fig. 7 shows the internal circuit structure of the combination component Q of Hasan finite-field multiplier illustrated in Fig. 6.

Fig. 8 shows a completed function module of the conventional Hasan finite-field multiplier.

Fig. 9 is a circuit diagram of the internal components of a Hasan finite-field multiplier illustrated in Fig. 8.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The general finite-field multiplier and the method of the same according to the present invention will be described in the following with reference to the finite-field multiplying operation of $C = A * B \mod p(x)$ illustrated in equation (1). Based on the parallel multiplier algorithm disclosed by Mastrovito, A is first expressed in a matrix form by the relation of each element with the p(x), and then matrix-multiplied with B so as to generate the value of matrix C.

$$
\begin{aligned}
C = AB \quad &\mod p(x) \\
&= b_0 A + b_1 (A\alpha \mod p(x)) \\
&+ b_2 (A\alpha^2 \mod p(x)) + \text{.......} \\
&+ b_{m-1} (A\alpha^{m-1} \mod p(x)).
\end{aligned}
\qquad (1)
$$

$$C = AB \quad \mod p(x)$$
$$= b_0 A + b_1 (A\alpha \quad \mod p(x))$$
$$+ b_2 (A\alpha^2 \quad \mod p(x)) + \ldots\ldots$$
$$+ b_{m-1}(A\alpha^{m-1} \quad \mod p(x)). \tag{1}$$

It is known from equation (1) that when two finite-field elements are multiplied, at first, each bit in element A can be expanded through an XOR operation, and the expansion value is performed an AND operation with each bit in element B for generating the value of element C. Therefore, the form of the Mastrovito multiplier is related to a non-reducible polynomial p(x). Therefore, the matrix form expanded from the equation (1) is given as follows:

$$\alpha^m = p_{m-1}\alpha^{m-1} + p_{m-2}\alpha^{m-2} + \Lambda + p_{m-1}\alpha + 1 \tag{2}$$

$$\begin{vmatrix} A & A\alpha & \Lambda & A\alpha^{m-1} \end{vmatrix} \bullet b = c \tag{3}$$

$$A\alpha^k = A^{(k)} = A^{(k-1)}\alpha \quad \mod p(x) \tag{4}$$

$$A^{(k)} = a_{m-1}^{(k-1)}\alpha^m + a_{m-2}^{(k-1)}\alpha^{m-1} + \Lambda + a_0^{(k-1)}\alpha \tag{5}$$

$$a_i^{(k)} = \begin{cases} a_{i-1}^{(k-1)} + a_{m-1}^{(k-1)}p_i & 1 \le i \le m-1 \\ a_{m-1}^{(k-1)}, & i=0 \end{cases} \tag{6}$$

$$\begin{bmatrix} a_{m-1}^{(0)} & a_{m-1}^{(1)} & \Lambda & a_{m-1}^{(m-1)} \\ a_{m-2}^{(0)} & a_{m-2}^{(1)} & \Lambda & a_{m-2}^{(m-1)} \\ M & \Lambda & \Lambda & M \\ a_0^{(0)} & a_0^{(1)} & \Lambda & a_0^{(m-1)} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ M \\ b_{m-1} \end{bmatrix} = \begin{bmatrix} c_{m-1} \\ c_{m-2} \\ M \\ c_0 \end{bmatrix} \tag{7}$$

Therefore, it is known that the primary principle of a parallel multiplier is to make one of two multiplied elements into a matrix form

for being performed with a vector operation with the second element so as to generate a desired value. The matrix form is illustrated in equation (7). The equation (8) is a matrix form simplified according to an equation $p(x)=1+x+x^4$. The operation is $A \times B = C$, where A, B and C are finite-field elements. Therefore, it is known that the primary circuit elements of the parallel multiplier are AND gates and XOR gates. With the increasing of the highest order of the p(x), i.e. the increasing of the value of m, the complexity of the hardware thereof is about $O(m^2)$.

$$\begin{bmatrix} a_3 & a_2 & a_1 & a_0 + a_3 \\ a_2 & a_1 & a_0 + a_3 & a_2 + a_3 \\ a_1 & a_0 + a_3 & a_2 + a_3 & a_1 + a_2 \\ a_0 & a_3 & a_2 & a_1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{bmatrix} \qquad (8)$$

According to Mastrovito multiplier equation (7), it is known that the vector in the second column vector is generated from various p(x)'s and first column vector. The other column vectors can be obtained in the same manner, and thus the values in the matrix of equation (7) can be generated. Therefore, a multiplier designed in a serial connection manner can effectively reduce the cost and area thereof, while the operation speed will be slowed down. Therefore, in the present invention, the parallel operation in VLSI implementation is employed to quickly obtain the result of the multiplication of two finite-field elements.

According to equation (6), each column matrix in equation (7) can be derived by the values of the previous column and the coefficients of p(x). The equation (6) is simplified to have the equation (9). From equation (9), the vector values of each column can be obtained. From

equation (9), it is known that the values of the k-th column are only related to the (k-1)-th column and the coefficient of the p(x). In the relation, the (k-1)-th column must be at first shifted. Then, the shifted last bit value $a_{m-1}^{(k-1)}$ and p(x) are AND-ed, and the result is XOR-ed with a
5   displaced value for generating a matrix of the k-th column. The relation is illustrated in equation (9).

$$a_0^{(k)}=a_{m-1}^{(k-1)}$$
$$a_1^{(k)}=a_0^{(k-1)}+a_{m-1}^{(k-1)}p_1$$
$$a_2^{(k)}=a_1^{(k-1)}+a_{m-1}^{(k-1)}p_2$$
$$\mathbf{M}$$
$$a_{m-1}^{(k)}=a_{m-2}^{(k-1)}+a_{m-1}^{(k-1)}p_{m-1} \qquad (9)$$

Based on the matrix A induced from equation (9), the primary principle, i.e. the features, among the columns can be known. Equation
10   (10) shown the arrangement of matrix A. In brief, the relation of the first column and the second column is that the values of the second column is derived from the first column by shift each value in first column upwards through one element in the matrix. That is, the value of $A_{0,0}$ in the second column is shifted to the position of $A_{m-1,1}$ in the second column,
15   while the values originally in $A_{1,0} \sim A_{m-1,0}$ are shifted one position to the positions of $A_{0,1} \sim A_{m-2,1}$ in the second column, respectively. Then, according to the coefficient of p(x), it is determined whether to add the value original in $A_{0,0}$ to $A_{0,1} \sim A_{m-2,1}$. When the coefficients of p(x) with respect to the $A_{0,1} \sim A_{m-2,1}$ are 1's, then values in $A_{0,0}$ $A_{0,1} \sim A_{m-2,1}$ are
20   added thereon. For example, if the coefficient of p(x) at position $A_{0,1}$ is 1,

10

then $A_{0,1} = A_{0,0} + A_{0,1}$, while the value at $A_{0,0}$ is placed at the position of $A_{m-1,1}$. Thus, the values of the second column are obtained. The same process is used to derive the relation between the second column and the third column, the relation between the third column and the fourth

5   column, etc., until all the columns in the matrix are derived.

$$A = \begin{bmatrix} A_{0,0} & A_{0,1} & \Lambda & A_{0,m-1} \\ A_{1,0} & A_{1,1} & \Lambda & A_{1,m-1} \\ M & M & O & M \\ A_{m-1,0} & A_{m-1,1} & \Lambda & A_{m-1,m-1} \end{bmatrix} \qquad (10)$$

Therefore, the relations among the columns can be acquired from aforesaid description. Furthermore, from the multiplication equations of the finite-field elements, it is known that the vector multiplication

10   operation must be used for the multiplying two elements. Therefore, the XOR gates and AND gates are required, and thus the circuit for the finite-field multiplier of the present invention is derived. Referring to Fig. 1, there is shown the structure of the finite-field multiplier according to a preferred embodiment of the present invention, which includes a parallel

15   column-based matrix vector generator 11 and a parallel column-based vector multiplication operator 12. The circuit structure of the finite-field multiplier is illustrated in Fig. 2. Such a circuit is designed by utilizing equation (9), wherein the circuit component for generating the matrix A is the parallel column-based matrix vector generator 11, which has

20   flip-flops 111 provided primarily for latching the elements in each column of the matrix A generated by the parallel column-based matrix vector generator 11. The multiplexer MUX is provided to decide which

11

bit will be shifted out so as to determine the size of the matrix A. The AND gate is provided to determine whether the shifted value will be added to the elements of the next column. The multiplication operation is performed by the XOR gate 113. The generated column elements of the matrix A are then transferred to the parallel column-based vector multiplication operator 12. In this circuit, the flip-flop 121 is provided to latch the multiplying results of the elements in each column of the matrix A with the elements of the vector B. Then, the result is accumulated to the multiplying results of the elements in each column of the matrix A with the elements of the vector B. After m time of accumulating operations are performed, the desired vector C is generated. The circuit is characterized in that only one multiplexer is used to determine the bit for being shifted out. Therefore, the whole multiplication circuit is provided with a programmable bit number of the finite-field element, so that the number of bits generated in each column of the matrix A has a minimum of 2 and a maximum of m. Furthermore, the p(x) can be changed by an external input for matching the requirements of different specifications.

Fig. 3 shows a structure of another preferred embodiment of the finite-field multiplier according to the present invention implemented by the equation (9), which includes a parallel matrix vector generator 31 and a plurality of parallel vector multiplication operators 32. The circuit structure of the finite-field multiplier is illustrated in Figs. 4 and 5. The parallel matrix vector generator 31 is primary used to generate a matrix A. The basic circuits for each column are denoted by block 2 ~ block m, which generate the elements in each column of the matrix A, respectively.

Similarly, after the matrix A completes the operation, the results are sent to the parallel vector generator 32. Then, the vector values of n-th row of matrix A are operated with the elements in vector B to acquire each element of the vector C. Finally, after all the elements are determined, the

5   vector C is obtained. The difference of this embodiment from the conventional multiplier is that a parallel operation is used in the present invention and only m-1 multiplexers (MUX) are used to determine which bit is required to be shifted out. Therefore, the number of bit in each finite-field element can be determined so that the whole circuit of the

10 multiplier becomes a multiplier circuit with a programmable bit number of finite-field element, and the p(x) can be changed by an external input. The matrix A has a minimum size of 2×2 and a maximum size of $m \times m$. In view of the foregoing, it is known that, in the general finite-field multiplier and the method of the same according to the

15 present invention, the AND gates and XOR gates are primary components, and the input signals includes elements of the matrix A and the vector B and the coefficients of the polynomial p(x). When A, B and the coefficients of p(x) are input, the elements in vector C can be obtained rapidly. The major difference of the present invention from the

20 conventional multiplier is that, in the present invention, the inputs contain multiple bits, and the multiplication operation is performed with multiple bits. Therefore, it is very convenient to be integrated with an existing communication system. Accordingly, the multiplier can be used in an RS chip for different specifications.

25   Although the present invention has been explained in relation to

its preferred embodiment, it is to be understood that many other possible modifications and variations can be made without departing from the spirit and scope of the invention as hereinafter claimed.